Authentication on Internet of Things(IoT)

Mtech thesis work done by

Mente Sindhu

Roll No: 213CS1147

Master of Technology

in

Computer Science

under the supervision of

of

Prof. Ashok Kumar Turuk

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769008, India

Authentication on Internet of Things(IoT)

a thesis submitted in partial fulfillment of the requirements

for the degree of

Master of Technology

in Computer Science and Engineering

by

Mente Sindhu

(Roll. 213CS1147)

under the supervision of

Prof. Ashok Kumar Turuk

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769008, India

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India.

Certificate

This is to certify that the work in the thesis entitled " ***Authentication on Internet of Things (IoT)*** " submitted by ***Mente Sindhu***, bearing RollNo. ***213CS1147***, is a record of an original research work carried out by her under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Science and Engineering, National Institute of Technology, Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Dr.Ashok Kumar Turuk
Assistant Professor
Department of CSE
National Institute of Technology
Rourkela-769008

Place: Rourkela
Date: 25 - 05 - 2015

Acknowledgment

I have taken efforts and interest for doing this project. I have learnt many important things about IoT and RFIDs during the project. However, this might have not been successfully completed without the kind help and support of many people and my organization. I would like to sincerely thank each and every one of them.

First of all, I would like to thank my respected supervisor Dr. Ashok Kumar Turuk from the bottom of my heart, for his perfect guidance and constant supervision through out the project. He always guided me by showing the right path to follow at every step to successfully complete my project. I would like to express my deep sense of gratitude to him for providing me all the necessary data and material required for the project. I am greatly indebted to him for his encouragement and invaluable advice not only in my project but also in all aspects of my academics through out my stay here.

I would like to express my special gratitude and thanks to our respected head of our department, Dr.S.K.Rath, Dr.B.D.Sahoo, Dr.K.Sathya Babu and other faculty members for giving good advice and encouraging me through out the project.

I am also very thankful to my organization for providing me with all the required resources, good laboratory facilities needed for the research work.

I would also like to thank all my friends who helped me during the course of the project.

Lastly, I would like to convey my heartful thanks to my parents, for giving me this wonderful opportunity to study in this college,and for their constant encouragement and support.

Sindhu Mente

Abstract

Internet of Things (IoT) is a rapidly growing technology that is gaining importance in the area of ubiquitous computing. The main aim behind this concept is to provide communication capabilities to all the things present around us, so that these devices can communicate directly among themselves in an intelligent manner eliminating the need for human intervention. This communication is established by the use of RFID tags, sensors etc., which are provided with addresses to be uniquely identified and to communicate with each other. The main problem with IoT is providing security and privacy. Among many wireless technologies used for communication among devices, RFID technology is the most popular and widely used. Various factors like reduction in terms of size, weight, energy consumption lead to its popularity. So, in this thesis we mainly concentrate on RFID and its security problems. Since, RFID is a wireless communication technology; it is very easily prone to attacks and intrusions from the adversaries. So, we have to develop strong authentication algorithms which provide maximum security so that this technology can be used for the implementation of Internet of Things. But, the problem is that, RFID tags consist of very low tag resources in terms of memory and computational capabilities. It is very difficult to develop authentication protocols that consume minimum tag resources and provide maximum security. So, our goal is to develop lightweight authentication protocols which use simpler operations like XOR, Rot etc. which consumes very few tag resources and aims to provide maximum security.

***Keywords*:** IoT, RFID, Ubiquitous computing, Security and privacy

Contents

List of Acronyms

Acronym	Description
IoT	Internet of Things
RFID	Radio frequency Identification
LMAP	Lightweight Mutual Authentication protocol
M^2AP	Minimalistic mutual authentication protocol
SASI	Secure Authentication and Secure Integrity Protocol
RAPP	RFID authentication protocol with Permutation
SIDRFID	Static Identifier RFID authentication protocol
DIDRFID	Dynamic Identifier RFID authentication protocol

List of Figures

List of Tables

Chapter1

Introduction

Internet of Things(IoT) is the connection between devices, which can be uniquely identified through the IP addressing scheme and which have the capability to communicate with other devices to attain the required objectives. IoT strives for providing the ability to the interconnected devices in a network to transfer data without the need of human-human interaction or human-machine interaction. It aims to provide services directly based on machine-machine interaction.

1.1 Need for IoT

In today's world, the Internet and the computers for the most part are dependent on people for data. Most of the information introduced in the web today was once captured or accumulated by individuals and accordingly made by them by either writing, taking computerized pictures or by reading standardized tags. The problem with this is that individuals have restricted time, consideration and precision which implies that they are bad at capturing information about things in a certifiable manner. Thus, if computing gadgets have the capacity to capture information from the gadgets directly and disregard it to the web with no human intervention, then precision and quality of information is enhanced and waste, loss and expenses are lessened.

Internet of Things is not simply being connected as far as PCs, advanced mobile phones, tablets and so on. It portrays a world where anything can be connected and made to interact in a intelligent manner. In this way, for the effective execution of the Internet of Things where millions or billions of knowledgeable devices are associated,

the first step is changing over systems on restrictive conventions to IP based systems. The present IPV4 addressing system which is being currently used for identifying the computing devices will not be sufficient for the implementation of the IoT. We need to shift to IPV6 addressing system which is 128-bit addressing and can be easily used to address the billions of things that are going to be connected.

1.2 Applications of IoT

There are many important applications provided by IoT. A few of them as listed by Rolf H.weber [13] are as follows:

- Transportation
- Logistics
- Health care
- Smart environments
- Security applications

1.3 RFID

RFID is a very popular technology used for identification of objects automatically through Radio signals. The deployment of the RFID technology requires the following three components.

- RFID Tag
- RFID Reader
- Backend Server/database

1.3.1 RFID tags

RFID tags are mounted on the objects which are to be supervised. They are mounted with small IC's which contains an ID that can be used to uniquely identify the item to which it is attached. Each tag in an RFID system has a specific amount of memory internally, where the information concerned to the object can be stored. RFID tags come in different varieties namely:

1. Read-only tags 2. Write Once Read Many (WORM) tags
3. Read/Write tags.

Tags classification according to resources is as:

1.Passive 2. Semi passive 3. Active tags.

- **Passive tags:**
  1. They don't have an internal clock and own power supply and depend on the radio signals transmitted by the readers for their operation.
  2. These tags are generally cheap.
  3. The resource constraints like no self power source, very less internal memory make them operationally challenging.
- **Semi passive tags:**
  1. They have internal battery power for performing computations but they rely on the power from the signal transmitted by the reader for transmission of messages.
  2. Prices are moderate.
- **Active tags:**
  1. They have their own internal clock, power supply and large internal memory.
  2. These tags are generally costly.
  3. They have no resource constraints.

RFID technology is gaining importance in the widespread implementation of IoT. The success of this technology depend on gaining public acceptance, which requires addressing the privacy and security problems hindering the usage of RFID tags.

1.4 Types of RFID systems

RFID systems are segregated depending on the range of frequencies with in which they operate as:
1. Low frequency 2. High frequency 3. Ultra high frequency:

- **LF RFID**
  - Low Frequency RFID applications work in the range of 125KHz - 132.5KHz.
  - It has a short read range of approximately 10cms.
  - Data read speed is very low in these RFIDs.
- **HF RFID**
  - High frequency RFID systems operate in the frequency range of 3-30MHz.
  - They have more data transfer rate compared to Low frequency RFIDs
  - Read range is between 10cm-1m.
- **UHF RFID**
  - Ultra High Frequency RFID applications operate at very high frequencies ranging between 860MHz-960MHz.
  - The data transfer rates are the highest in these RFIDs.
  - The data read ramge is as high as 12m.

1.5 Working of RFID

An RFID system typically consists of these three important parts namely: A scanning antenna, a transceiver at the reader side to decode the information on the tag and a

transponder that is mounted on the RFID tag and is programmed with some data. The RFID tags used in the system may be provided with a power supply or may not be provided. Tags containing their own power supply have lesser life span because they become inactive after the battery is depleted. The tags not having the power supply have longer life spans. They take the power from the power signal from the scanner. The scanners can be either fixed at a particular location,handheld or movable. They can assume any shape and size depending on the application.

When a transponder of a RFID tag is made to pass through the radio frequency signals of the scanner, the transponder at the tag gets activated,authenticates the scanner and then transfers all its data to the transceiver. The transceiver decrypts the data and then processes the data according to the application.

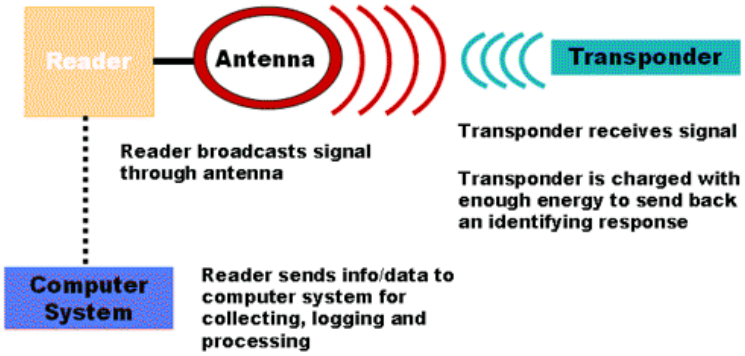


Figure 1.1: RFID working

1.6 Security threats to RFID Applications

- **Eavesdropping:** The attacker stores all the messages transmitted between the sender and the reader and later does cryptanalysis of the messages stored.
- **Replay attack:** The adversary stops the actual messages in the communication and instead sends the messages eavesdropped in the previous sessions to spoof as a valid tag or a reader.

- **Cloning:** Cloning is the process of reading all the information that is stored in a valid tag and then writing the same onto another blank tag and use it as a valid tag.

- **Tag tracing:** The process by which the attackers identify the location of the tag either by communicating with it or by analysis of messages stored passively is called tag tracing.

- **Invading privacy:** It means finding the information about the user without his knowledge. For example, in a shopping transaction, finding what all items the customer had purchased.

- **Data forging:** The modification of the critical information on the tag like product price on the tag by the adversary is called data forging.

- **Denial of Service:** The prevention of the tag and reader to communicate with each other.

- **De synchronization:** Modifying the secret information like keys shared by the tag and reader, so that the keys between them do not match and consequently the authentication process between them fails.

1.6.1 Physical mechanisms for RFID security

- **Kill Codes:** It is a method of permanently deactivating the tag. The codes on the tag are killed and the tag becomes unresponsive to reading and tracing. This approach is generally employed when the tracking of the object to which the tag is attached is no longer required.

- **Faraday Cage:** By this method, the user can decide when he wants the tag to be traceable. If the tag should not be traceable,then it is put in a faraday cage. The faraday cage is built with a material that do not permit the electromagnetic waves to pass through it. As a result, the tag cannot be tracked.

- **Blocker Tag:** The blocker tag prevents access to the unauthorized users by creating an illusion that many other RFID tags are present. It jams the signal

going to the actual tag from the reader. It is generally placed near the actual tag.

1.7 Types of RFID Authentication

Authentication protocols are mainly classified into four different types as follows:

1. Ultra light weight
2. Light weight
3. Simple
4. Fully secured

- **Ultralight weight:** Uses only simple bitwise operations at the tag side.
- **Light weight:** Uses simple functions like CRC ,Psuedo random number generator functions and bitwise operations.
- **Simple:** Uses hash functions along with the previously described operations.
- **Fully secured:** Can make use of any complex functions irrespective of the resources they demand, but finally provide maximum security.

1.8 Motivation

Internet of Things (IoT) has recently become a buzz word among the computer scientists. Its applications are growing day by day. The idea behind this technology is to interconnect all the things existing around us and allowing them to interact among themselves and exchange data. The problem for its full scale implementation is the privacy and the security problems it is facing. The users can be tracked without even being known that they are tracked. The things are provided with sensors mainly RFIDs that capture the data. The sensors transfer the data to their readers. So, to provide privacy, an authentication scheme must be established between these sensors and the readers. This method ensures the required security and the privacy, but sophisticated cryptography which we use for normal authentication cannot be used here because the RFID tags used for sensing are constrained with limited resources.

1.9 Objective of Research

The main objectives we find from the motivation to work in the area of "Authentication on IoT" are discussed as follows:

- **Security Problem:** To design such a robust authentication protocol which is secure against all known security breeches.
- **Minimum resources:** As the Passive RFID tags are resource constrained, the authentication protocol should consume minimum storage and computational resources.

1.10 Organization of the Thesis

The organization of the rest of the thesis is as described below:

1. **Chapter 1:** In this chapter, we have discussed about the introduction to Internet of Things,RFID technology and security and privacy issues associated with them, motivation and objective of my research.
2. **Chapter 2:** In this chapter, we present the literature survey where I have discussed some of the pre- existing RFID mutual authentication protocols and the analysis of their security.
3. **Chapter 3:** In this chapter, we discuss about my proposed new RFID authentication protocol and improvements to few of the existing protocols to protect them from various security attacks.
4. **Chapter 4:** In this chapter, we show the implementation of the protocol and analyze its security with the help of an automatic protocol verification tool known as SPAN.
5. **Chapter 5:** In this chapter, conclusion, future scope of the research work done are given.

CHAPTER2

Literature Survey

Over the past few years, many protocols have been proposed that claimed to prevent the vulnerabilities against authentication between the RFID tag and the reader but have failed. The summary of few of these protocols is as follows:

2.1 LMAP RFID authentication protocol

This protocol is proposed by Peris-Lopez [14] in 2006. It is makes use of the Index Pseudonyms(IDS). IDS is a 96 - bit index used for retrieving all the information corresponding to a particular tag from database of the reader or a back end server. The keys shared between the tag and the reader are divided into 4 parts K1, K2, K3, K4 each of 96 - bit length.
In this protocol, the reader does the expensive operations like hash,random number generation etc., while the tag which is constrained with resources, only performs simple operations on bits like XOR, OR, AND and (2^m) modulo addition. The protocol works in the following fashion:

$A = IDS \oplus K1 \oplus n1$
$B = (IDS \vee \text{K2}) + n1$
$C = (IDS + K3 + n2)$
D = IDS+ID $\oplus$ $n1 \oplus n2$

IDS and Key updating:
$IDS^{new} = (IDS + (n2 \oplus K4)) \oplus ID$

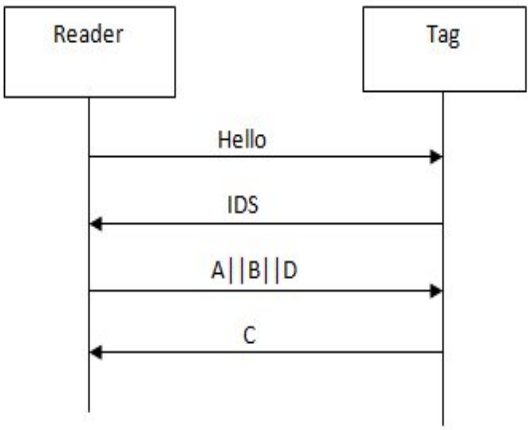


Figure 2.1: LMAP authentication protocol

$K1^{new} = K1 \oplus n2 \oplus (K3 + ID)$
$K2^{new} = K2 \oplus n2 \oplus (K4 + ID)$
$K3^{new} = K3 \oplus n1 + (K1 \oplus ID)$
$K4^{new} = K4 \oplus n1 + (K2 \oplus ID)$

2.1.1 Drawbacks of LMAP

This protocol is prone to the following attacks as proposed by G.Avione [6]:

1. Full disclosure attack.
2. De synchronization attack.

2.2 M^2AP RFID authentication protocol

M^2AP is a RFID mutual authentication protocol also proposed by Peris-Lopez [9]. This protocol was assumed to provide the required amount of security by consuming very few resources on the tag. It requires approximately 300 logic gates. The various phases in this protocol are:

- Tag singulation.
- Mutual authentication.

- IDS updating.
- Key updation.

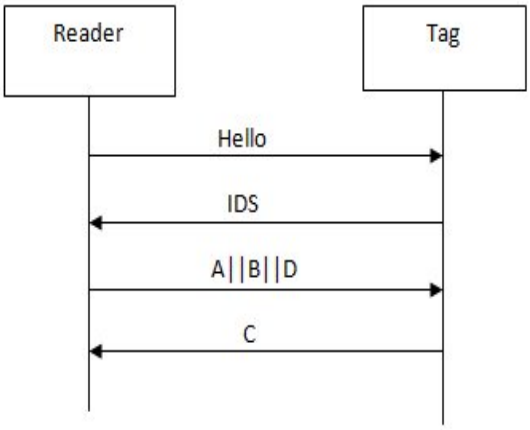


Figure 2.2: M^2AP authentication protocol

2.2.1 Drawbacks

1. Each bit is affected only by the bits which have same or higher index. So the least significant bits are independent of the other bits in the messages.
2. This protocol also uses OR and AND bitwise operations whose result is not equally probable. The result of AND operation can be 0 and the result of OR operation can be 1, each with a probability of (3/4). The use of these non-triangular operations makes it prone to tango attack.
3. From the messages B and D, the information about the random numbers n1 and n2 can be easily acquired, with the help of 1's and 0's in the IDS.
4. The 2^{96} modulo addition can be easily cracked if every bit on the right hand side is known.

2.2.2 Possible attacks

1. Tracing: If the messages of two consecutive sessions of the protocol are eavesdropped, the attacker can easily find the value of ID and can trace it.
2. Tag impersonation.
3. Reader impersonation.

2.3 SASI mutual authentication protocol

This Ultralight weight authentication protocol is proposed by Y.Chien in 2007 [10].Ultra lightweight protocols refer to the family of protocols that involve only simple bitwise operations like OR, AND, XOR, rotation etc. on tags. Ultra light weight mutual authentication protocols are very useful for passive RFID tags because they have very few internal resources.

2.3.1 Drawbacks

SASI is an ultra light weight authentication protocol, which is aimed to provide strong authentication and integrity. The protocol suffers from the following attacks as described by W.Phan [11].

1. De-synchronization attack which breaks the synchronization between the reader and tag by enabling wrong computation of secrets at either of them.
2. Identity disclosure attack, through which the tag ID can be determined.
3. Full disclosure attack, through which all the secret data like the keys can be retrieved.

2.4 Gossamer protocol: An advancement to the ultra light weight cryptography

This protocol is designed by Peris-Lopez [12] with inspiration from SASI protocol. It aims to be devoid of the security weaknesses of the SASI protocol. It can be employed

in passive RFID tags for which ultra lightweight cryptography is the most efficient.

2.4.1 Drawbacks

The weaknesses of Gossamer protocol described by Bilal [8] included the use of unbalanced logical operators. The vulnerabilities discovered from the analysis conclude that many attacks like denial of service (DoS), de-synchronization, replay of messages, data integrity violation and Index Pseudonym collision attacks are possible. Moreover, it is computationally exhaustive.

2.5 RAPP:New ultralight weight RFID authentication protocol using Permutation

RAPP is new ultra light weight RFID authentication protocol proposed by Y.Tian [1]. RAPP avoids the use of unbalanced triangular operations like bitwise OR and AND and introduces a new operation called permutation. RAPP uses very less tag resources like computation power, storage requirement and the cost for communication. In RAPP, tags involve mainly three operations:

- Bitwise XOR
- Left Rotation Rot()
- Permutation Per()

If X and Y are two strings of length 'l' and the number of 1's in Y, $wt(Y) = m$ then,
$y_{k1} = y_{k2} = ... = y_{km} = 1$
$y_{km+1} = y_{km+2} = ... = y_{kl} = 0$
$Per(X, Y) = x_{k1}\ x_{k2}. . . . .x_{km}\ x_{kl}\ x_{kl-1}. . . . . .x_{km+2}\ x_{km+1}$

The permutation operation can be performed as follows:

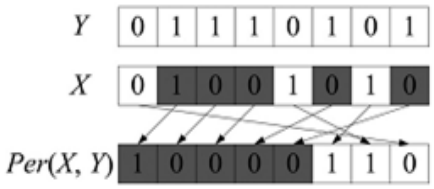


Figure 2.3: Permutation operation

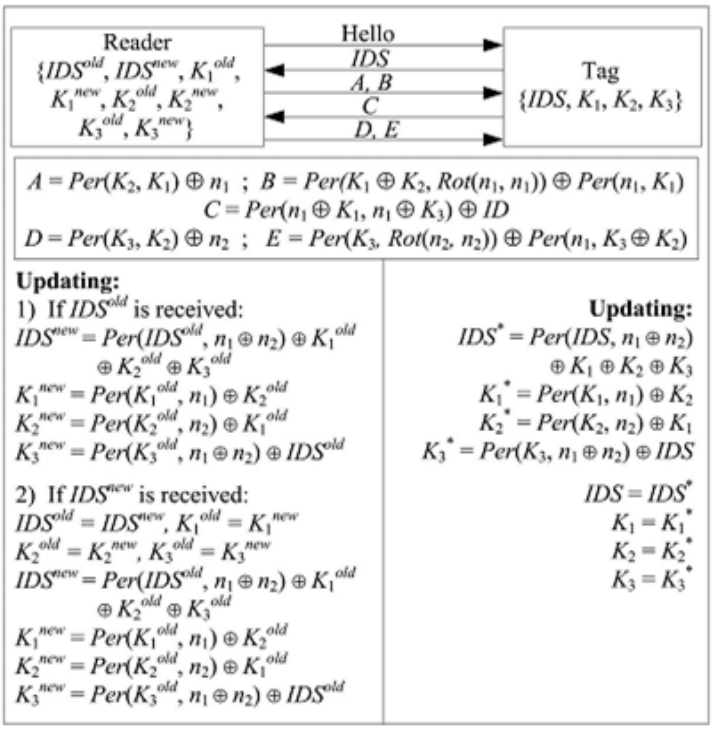


Figure 2.4: RAPP authentication protocol

2.5.1 Drawback

This protocol suffers from the following security attacks as described by Z.Ahmadian [2]:

- De synchronization attack
- Traceability attack
- Full disclosure attack

2.6 Improved RAPP authentication protocol

This paper is modified from RAPP by Xinying Zheng [21] with the objective to eliminate all the weaknesses of RAPP while reducing the computational and communicational complexity.

$n1 = f(K_1, r)$

$n2 = f(r, K_2)$

$B = per(K_2 \oplus n_1, Rot(n_1, n_1)) \oplus per(n_1, n_1 \oplus k_1)$

$C = per(n_2 \oplus, n2 \oplus K_2) \oplus ID$

Key Updating Process:

$IDS^{new} = per(IDS, n1 \oplus n2) \oplus K1 \oplus K2$

$K1^{new} = per(K1, n1) \oplus n1$

$K2^{new} = per(K2, n2) \oplus n2$

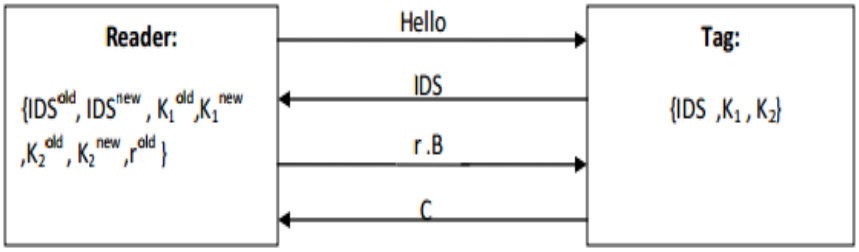


Figure 2.5: Improved RAPP authentication protocol

2.6.1 Drawbacks

This protocol shows reduced time and space complexities compared to the previous protocols and also resist the previously proposed attacks against $RAPP$. But this protocol is prone to IDS collision attack.

The reader generates the new tag pseudonym (IDS^{new}) after each successful protocol run, but it does not check if the generated IDS is already stored in the database

corresponding to another tag. So, if the collision of tag Pseudonyms occurs then the reader may fetch wrong values of keys and there is a possibility for the tag and the reader to get de-synchronized.

2.7 SIDRFID authentication protocol

This protocol is proposed by Lee Y.C [7].In this, the tag and the reader have identifiers IDT and IDR respectively, which are used in the authentication process. This protocol aims to consume minimum memory storage and computation requirements on the tag. The identifiers of the tag and the reader remain static in all sessions of the protocol. So, this type of protocols find uses in applications where one-time authentication is sufficient. The protocol working can be demonstrated as follows:

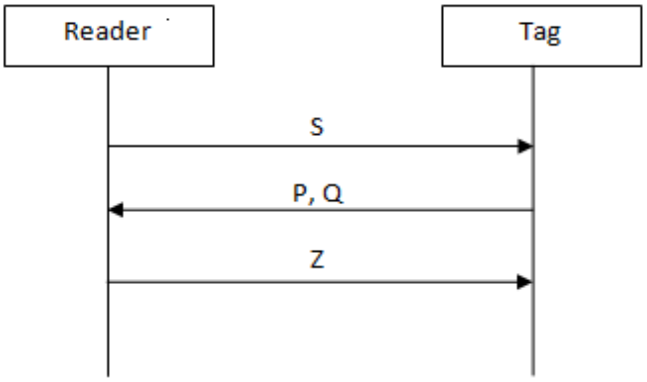


Figure 2.6: SIDRFID authentication protocol

$S = R \oplus IDR$

$P = IDT \oplus Rot(R, IDR)$

$Q = Rot(IDT, IDT) \oplus Rot(R, R)$

$Z = Rot(IDT, IDR \oplus R) \oplus Rot(IDR, IDT \oplus R)$

where R is the Random number and $Rot(x, y)$ is the circular left shift rotation operation by hamming weight(y) positions.

2.7.1 Drawbacks

The following are the drawbacks on SIDRFID authentication protocol [5, 6]:

1. **Passive hamming weight disclosure attack:** The hamming weight of IDR can be determined when the attacker eavesdrops two consecutive sessions of the protocol and obtain the values of S, P.

2. **Full disclosure attack:** This is an active attack where the attacker acts as an actual tag and sends messages to the reader. The attacker eavesdrops one round of the authentication and approximately 95 messages sent to the tag (if the key length is assumed to be 96 - bits)

2.8 DIDRFID authentication protocol

In this protocol proposed by Lee.Y.C [7], the tag uses an identifier $DIDT$ which gets updated after every successful authentication session. The tag and the reader shares a secret key K which is used for reader authentication by the tag. A random number R is generated by the reader which is used for tag authentication by the reader.
The protocol working can be demonstrated as follows:

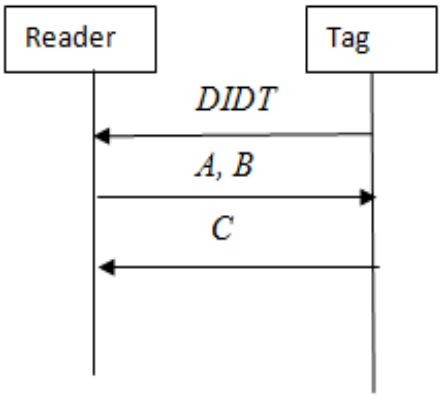


Figure 2.7: DIDRFID authentication protocol

$A = K \oplus R$

$B = Rot(K, K) \oplus Rot(R, R)$

$C = Rot(K, R) \oplus Rot(R, K)$

2.8.1 Drawbacks

The following are the weaknesses on DIDRFID authentication protocol [5]:

1. **Passive weight disclosure attack :** The attacker checks the messages B and C exchanged between the tag and the reader by eavesdropping them, until they are equal. If they both are equal hamming weight of R will be equal to hamming weight of K. By using the message A eavesdropped in two consecutive sessions of the protocol, their hamming weights can be easily determined.

2. **Traceability attack:** If the final message C sent by tag doesn't reach the reader, then the reader will not be able to update the $DIDT$ with the new value and thus allows the attacker to replay the values of A, B and consequently trace the tag.

2.9 Comparison of various authentication protocols

Parameter	LMAP	M^2AP	SASI	Gossamer	RAPP	Improved RAPP
Type of Computation operations	+,⊕,∨	+,⊕,∨,∧	+,⊕,∨,Rot	+,⊕,Mixbits	+,⊕,Rot	+,⊕,Rot
Storage requirement	6L	6L	7L	7L	5L	4L
Communication messages	2	3	2	2	2	2
Resistance to De synchronization attack	No	No	No	No	No	Yes
Resistance to disclosure attack	No	No	No	Yes	No	Yes
Resistance to tag tracking	No	No	No	Yes	No	Yes
Resistance to IDS collision attack	No	No	No	No	No	No

Table 2.1: Comparison of various authentication protocols in terms of security and resource requirements

2.10 SUMMARY

The following figure shows the summary of security of various authentication protocols [21]:

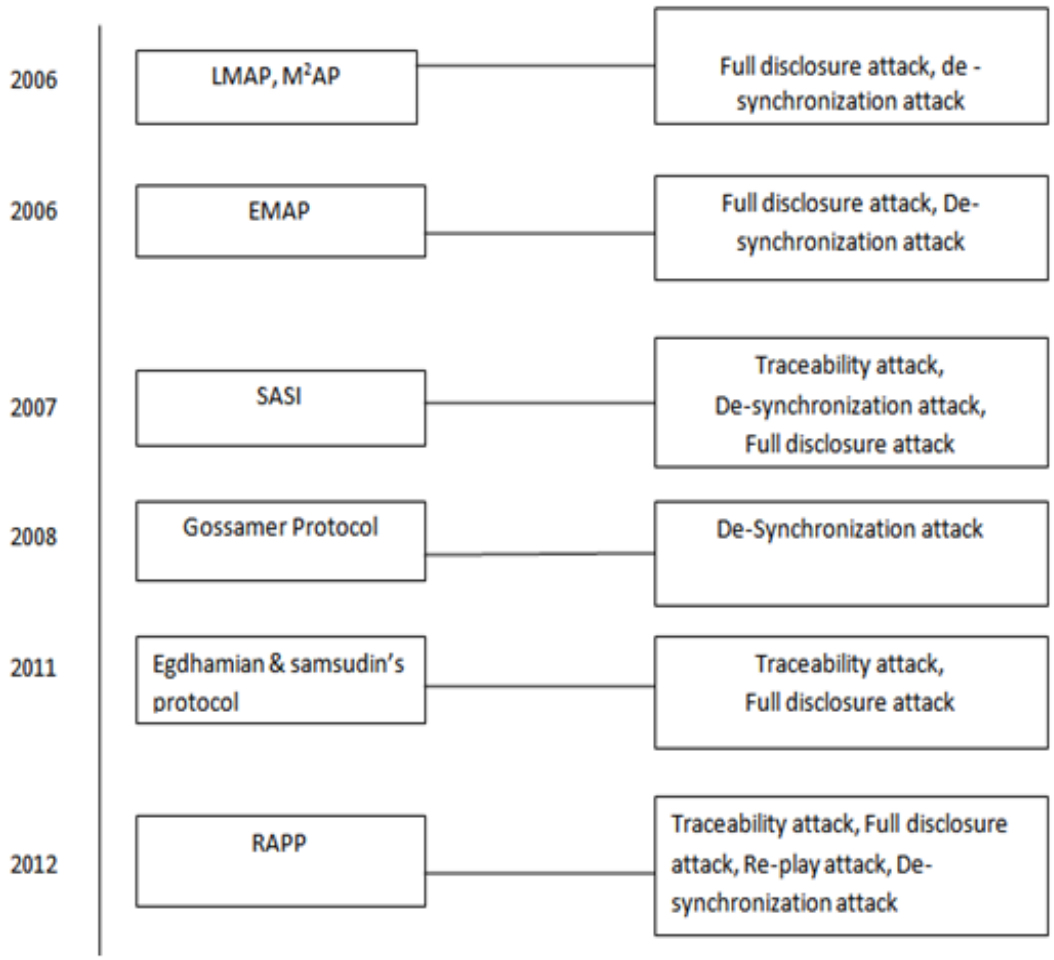


Figure 2.8: Comparison of various authentication protocols

CHAPTER3

Proposed Work

3.1 RFID mutual authentication protocol using shufflebits

3.1.1 Introduction

RFID is a fast evolving technology that is rapidly gaining importance in the area of ubiquitous computing which enables the smart devices to communicate anywhere. So providing security to the RFID system is very important. But the drawback with RFID systems is that, the low cost and low frequency RFID tags which are mostly used have very less resources associated with them. The resources can be computational or storage capabilities and battery power. Earlier many RFID mutual authentication protocols which are lightweight in nature, are proposed to serve this purpose. Most of them suffered from several security attacks. So, a new lightweight authentication protocol making use of simple operations like XOR, left circular rotation and shufflebits is proposed which aims to meet the security and privacy demands of the RFID system.

This proposed protocol mainly uses two bitwise operations namely:

1. OR 2. Shufflebits

The shufflebits operation internally uses the left circular shift operation.

The notations that are used in this protocol are as follows:

Symbol	Meaning
N_R	Reader generated Random number
N_T	Tag generated Random number
ID	Unique tag identifier
$K1^{old}$	Old value of key K1
$K1^{new}$	new value of key K1
$K2^{old}$	old value of key K2
$K2^{new}$	new value of key K2
A,B,C,D	Transmission messages used for authentication between the tag and the reader
$\ll$	circular left shift by mod(2^l) bits
wt(x)	No of bits containing '1' in x
$\oplus$	XOR operation

Table 3.1: Notations used in RFID protocol using shufflebits

3.1.2 Shufflebits() operation

Consider P and Q to be bit strings of lengths 'l'and 'l'respectively denoted as:

P = $\{p_1, p_2, p_3, p_4 \ldots p_l\}$

Q = $\{q_1, q_2, q_3, q_4 \ldots q_l\}$

Result: K = shufflebits(A)

```
1  s = 0, e =l,temp = 0,i = 1;
2  while i ≤ l do
3      instructions;
4      if ((P[ i ] ⊕ P[ i+1 ]) == 0) then
5          if ((temp == 0)) then
6              Q[ s++ ] = P[ i ];
7          else
8              Q[ e– ] = P[ i ];
9          end
10     else
11         if ((temp == 1)) then
12             Q[ e– ] = P[ i ];
13         else
14             Q[ s++ ] =P[ i ];
15         end
16     end
17     temp =P[ i ] ⊕ P[ i+1 ];
18     i++;
19 end
20 K = (Q ) ≪ Q mod (2^l );
```

Algorithm 1: Algorithm for Shufflebits operation

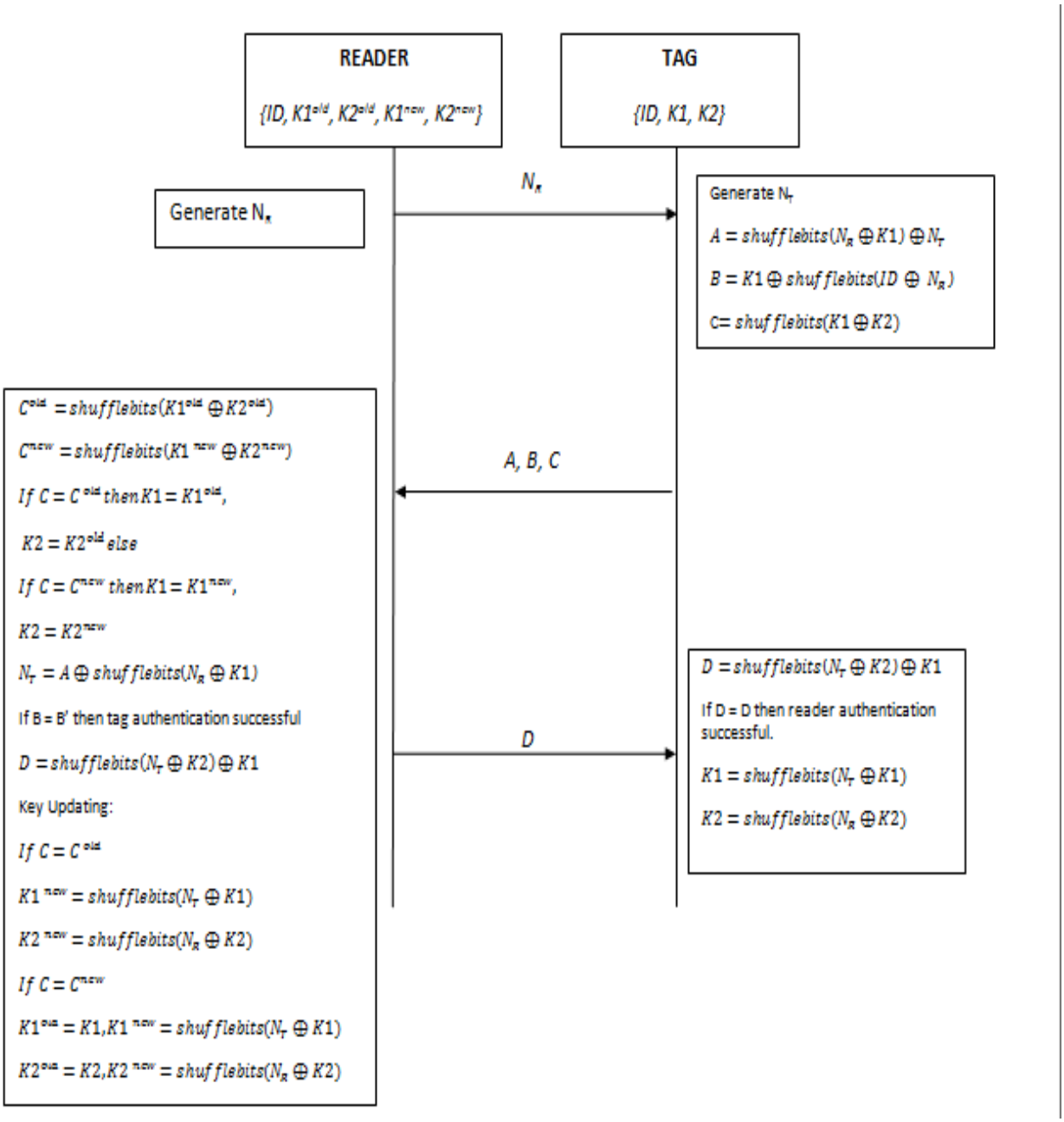


Figure 3.1: RFID mutual authentication protocol using shufflebits()

3.1.3 Detailed working of the protocol proposed

STEP 1: Consider a Reader and a Tag which stores {ID, $K1^{old}$, $K2^{old}$, $K1^{new}$, $K2^{new}$} and {ID, $K1$, $K2$} respectively.

STEP 2: Reader generates a random number N_R and sends it to the tag.

STEP 3: The tag calculates C = shufflebits($K1 \oplus K2$) and sends the value to the reader.

STEP 4: The reader then calculates C^{old} and C^{new} values and compares them with the received C value. If C matches with C^{old} then the old set of keys are used in the further authentication process. On the other hand if C matches with C^{new} then the new set of keys are used for further authentication where the values of C^{old} = shufflebits ($K1^{old} \oplus K2^{old}$) and C^{new} = shufflebits($K1^{new} \oplus K2^{new}$).

STEP 5: The tag also generates a random number N_T. The tag then calculates A and B values and sends them to the reader. A = shufflebits($N_R \oplus$ K1) $\oplus$ N_T, B = $K1\oplus$ shufflebits(ID$\oplus N_R$).

STEP 6: The reader then calculates N_T as, N_T = shufflebits($N_R \oplus K1$) and then calculates $B' = K1 \oplus$ shufflebits($ID \oplus N_R$). If the calculated B' and the received B are same then the tag authentication by the reader is successful. The reader then calculates D = shufflebits($N_T \oplus K2$) $\oplus$ $K1$ and sends it to the tag. The reader then updates its key values as :
If $C = C^{old}$ then $K1^{new}$ = shufflebits($N_T \oplus K1$) and $K2^{new}$ = shufflebits($N_R \oplus K2$), otherwise if $C = C^{new}$ then $K1^{old} = K1^{new}$, $K2^{old} = K2^{new}$, $K1^{new}$ = shufflebits(N_T $\oplus$ $K1$) and $K2^{new}$ = shufflebits($N_R \oplus K2$).

STEP 7: The tag calculates D' = shufflebits($N_T \oplus K2$) $\oplus$ $K1$. If D' and the received D are same then the reader is successfully authenticated by the tag and it updates it key values as $K1$ = shufflebits($N_T \oplus K1$) and $K2$ = shufflebits($N_R \oplus K2$).

3.1.4 Analysis of security of the protocol proposed

Data security and Integrity of the message:

In the proposed algorithm data security is maintained and integrity of the message is attained since all the secrets used in the authentication protocol are never transmitted in plain text but in some encrypted form by shuffling the bits. In tag only its ID is fixed and the key value gets updated in every run of the protocol.

Mutual authentication:

The random number N_T generated by tag and the keys $K1$ and $K2$ are known only to tag and reader. In the authentication sub messages, bits of these messages are scrambled and sent. So, unless the attacker can guess these values, he cannot decipher the authentication sub messages. Guessing the secrets is also very tough because they are sent in encrypted form.

Tag anonymity:

The random values N_R, N_T and Keys differ for each authentication round of the protocol. The shufflebits() function shuffles the values of these bits and moreover, the tag ID is also not sent in plain text form. So, the tag remains anonymous to the attacker.

Prevention of tracing attack:

All the messages exchanged in this protocol use random values and the bits are also shuffled, which imparts a property of randomness to the exchanged messages also and makes them untraceable.

Protection against Replay attack:

The Random values used in the protocol makes the message values different for each run of the protocol. These random value N_T and the keys cannot be found out as N_R is shuffled and XORed with keys. So, the messages cannot be replayed.

Forward Security:

Messages captured in a particular authentication round cannot give any information about the secrets to be used in the next authentication round because, the updation process makes use of shufflebits() operation on the random numbers which is then XORed with secret keys.

3.1.5 Protection against Impersonation attack:

In the protocol, messages B and C are used for tag authentication and reader authentication respectively, the values of which cannot be guessed or modified. So, the protocol is secure against impersonation attacks.

Protection from De-synchronization attack:

In this protocol the reader stores the values of both old and new keys ($K1^{old}$, $K1^{new}$, $K2^{old}$, $K2^{new}$) to protect the protocol against de-synchronization attack. The tag sends Shufflebits($K1$, $K2$) to the reader at the beginning of the authentication. Based on the value of that, the reader can understand if the tag was able to update its value in the previous authentication round of protocol. If the tag is unable to update its keys then the reader makes use the old values of keys stored in database for further authentication.

3.2 Further Improvements to Improved RAPP authentication protocol

The Improved RAPP algorithm provides resistance against the De-synchronization, disclosure and tag tracing attacks, the original RAPP algorithm is prone to,but still one attack is remained un addressed by the authors, which is the IDS collision attack. The algorithm generates a new IDS at the end of each authentication round. But it fails to check if that IDS is already present in the database corresponding to another tag, which may lead to De-synchronization attack.
The different notations that are used can be described as follows:

Symbol	Meaning
IDS^{old}	Old Index Pseudonym used for identification of tag.
IDS^{new}	New Index Pseudonym used for identification of tag.
ID	Unique tag identifier.
$K1^{old}$	Old value of key K1.
$K1^{new}$	new value of key K1.
$K2^{old}$	old value of key K2.
$K2^{new}$	new value of key K2.
r, B, C	Transmission messages used for authentication between the tag and the reader.
$n1$	Reader generated random number
$n2$	Tag generated random number.
$per()$	permutation operation.
$Rot()$	Rotation operation.

Table 3.2: Notations used for Improved RAPP authentication protocol

3.2.1 Protocol working

The protocol run and the messages exchanged are as follows:

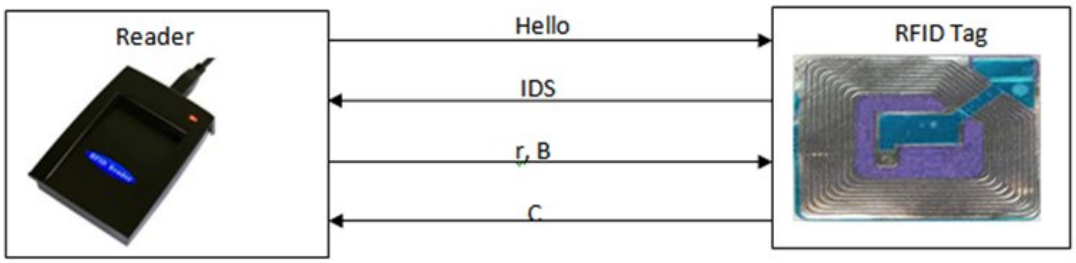


Figure 3.2: Improved RAPP authentication protocol

$$r = rot(per(ID, K1) \oplus n1, K2)$$
$$B = per(K2 \oplus n1, rot(n1, n1)) \oplus per(n1, n1 \oplus K2)$$
$$C = per(n2 \oplus K1, n2 \oplus K2) \oplus n1$$
$$n2 = per(K1, K2) \oplus n1$$

Updating:

$IDS^{old} = IDS^{new}$, $K1^{old} = K1^{new}$, $K2^{old} = K2^{new}$

$IDS^{new} = per(n1, n1 \oplus K1) \oplus K2$

$K1^{new} = per(K1^{old}, n2) \oplus K2^{old}$

$K2^{new} = per(K2^{old}, n2) \oplus K1^{old}$

$r^{old} = r$

3.2.2 Security Analysis

Resistance to IDS collision attack: In this modified protocol, we generate a new value for IDS using a random number and check in the database if it is already existing. If already existing, then a new value of IDS is generated and selected as the IDS for the next session of the protocol. So, the protocol can be protected from the IDS collision attack.

3.3 Improved SIDRFID authentication protocol

Lee proposed a static identity based RFID mutual authentication protocol known as SIDRFID authentication protocol. In this protocol,the tag and the reader are associated with identities namely IDT and IDR respectively. These identities remain fixed for all authentication rounds of the protocol. A random number R is generated by the reader. But, unfortunately this protocol is prone to various security attacks as described in the earlier chapter. So, we make slight modifications to this protocol to make it resistant to all the proposed security attacks.

In this protocol, we use a different function named Halfrot() instead of the Rot() function used in the original protocol. The halfrot() function works as follows:

Halfrot(X,Y)

Step 1: p = HW(X)+HW(Y)

Step 2: p1 = p mod(48)

step 3: p2 = 48-p1

Step 4: Left rotate X_L(Left half of message X) by p1 positions and left rotate X_R(Right half of message X) by p2 positions.

Step 5: Concatenate X_L and X_R after rotation.

The working of the protocol can be described as follows:

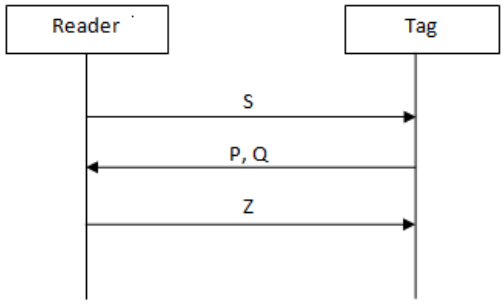


Figure 3.3: Improved SIDRFID authentication protocol

$S = R \oplus IDR$

$P = IDT \oplus Halfrot(R, IDR \vee R)$

$Q = Halfrot(IDT, IDT \wedge R) \oplus Halfrot(R \wedge IDT, R)$

$Z = Halfrot(IDT, IDR \vee R) \oplus Halfrot(IDR, IDT \wedge R)$

3.3.1 Step by Step working of the protocol

1. **STEP 1:**The reader generates the message $S = R \oplus IDR$ and sends it to the tag.

2. **STEP 2:**The tag generates the value R from message S as $R = S \oplus IDR$ and then calculates the messages P and Q.

3. **STEP 3:**The tag calculates the value of IDT from message P as IDT =P$\oplus Halfrot(R, IDR \vee R)$. Using the calculated IDT, it calculates Q value and checks if the received and the calculated Q are same or not. If they are not same, it means the attacker has modified the message and the protocol stops. If they are same then tag calculates the value of Z and sends to the reader.

4. **STEP 4:**The reader calculates Z value and compares it with the received value of Z.If both match,then the tag is authenticated by the reader

3.3.2 Security Analysis

Traceability: The traceability attack which is performed on the actual protocol is not possible in this protocol, because the rotation is not solely dependent on the hamming weight of the second parameter of the rotation operation.

Hamming weight Disclosure: The hamming weight cannot be disclosed by using the new Halfrot() operation.

Full Disclosure attack: Full disclosure of the secrets is also not possible. This is due to the failure to find the hamming weight of the secrets.

3.4 Improvement to DIDRFID authentication protocol

This protocol is also proposed by Lee, but unlike the previous one it has dynamic tag identifier $DIDT$ and Key K which keeps on changing for each successful authentication round of the protocol. But this protocol also suffers from traceability attack. So, we propose an improvement to this protocol. The message sequence in the protocol is as follows:

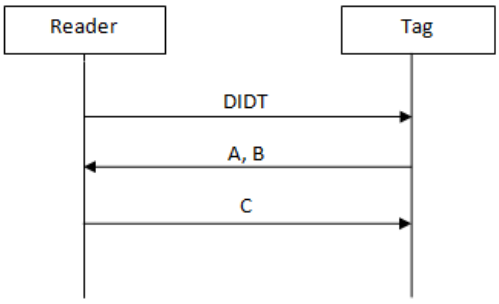


Figure 3.4: Improved DIDRFID authentication protocol

$A = K \oplus R$

$B = Halfrot(K, \sim K \vee R) \oplus Halfrot(R, R)$

$C = Halfrot(K, R) \oplus Halfrot(R, K \vee \sim R)$

Key updating:

$DIDTold = DIDT$

$Kold = K$

$DIDTnew = Halfrot(R, R \vee K) \oplus Halfrot(K, R \wedge K)$

$Knew = Halfrot(R, R \wedge K) \oplus Halfrot(K, R \vee K)$

3.4.1 Working of the protocol

1. **STEP 1:**The tag sends DIDT of tag to the reader.
2. **STEP 2:**The reader checks for DIDT in database and if it matches with the $DIDT^old$ then K^old is fetched, else if it matches with DID^Tnew, then Knew is fetched.The reader then calculates messages A and B and sends to the tag.
3. **STEP 3:**The tag calculates the value of R_T from message A as R =A$\oplus K$.Using the calculated K, it calculates B value and checks if the received and the calculated B are same or not. If they are not same, it means the attacker has modified the message and the protocol stops. If they are same then tag calculates the value of C and sends to reader.After sending C it updates its $DIDT$ and Key K.
4. STEP 4:The reader calculates C value and compares it with the received value of C.If both match,then the tag is authenticated by the reader and the reader updates its $DIDT$ and key K.

3.4.2 Security analysis

1. **Passive weight disclosure:**The hamming weight disclosure becomes impossible even if the messages exchanged are eavesdropped, because of the new Halfrot() operation.
2. **Full Disclosure:**The random number generated by the reader is calculated using message A and verified using message B. So, the random number cannot be modified by the adversary and the replaying of messages used for disclosure attack becomes impossible.

CHAPTER4

Simulation and Verification results

4.1 Simulation of New Improved RAPP mutual authentication Protocol

The old RAPP algorithm and the new RAPP authentication algorithm proposed to eliminate the IDS collision attack are implemented in java using client-server programming and using oracle as the backend database.
The comparison between the existing and the new protocol with respect to the resources required at the tag side are as follows:

Parameter	New RAPP	Improved RAPP
Type of Computation operations	11 XOR,6 per,1 Rot,2 PRF	10 XOR,8 per,2 Rot
Storage requirement	4L	4L
Communication messages	5	5
Resistance to IDS collision attacks	No	Yes

Table 4.1: Comparison of new RAPP and Improved RAPP authentication protocol

The following screen shots show how the former algorithm is prone to IDS collision attack and how the improved algorithm, which we proposed overcomes it by generating a new value of IDS and checking it across the database for prior existence corresponding to another tag.

The values of keys and IDS for one round of successful authentication between the tag and reader are as shown below:

In the old RAPP authentication protocol, when the IDS generated is already

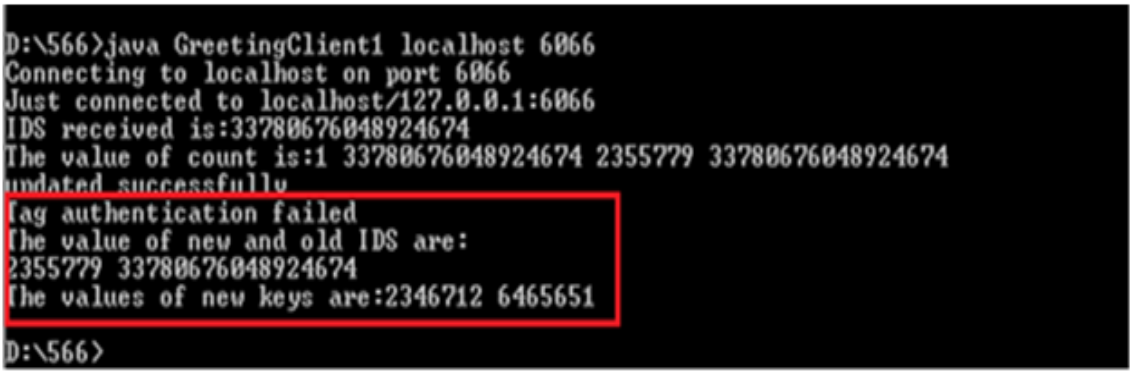


Figure 4.1: Modified RAPP Reader side

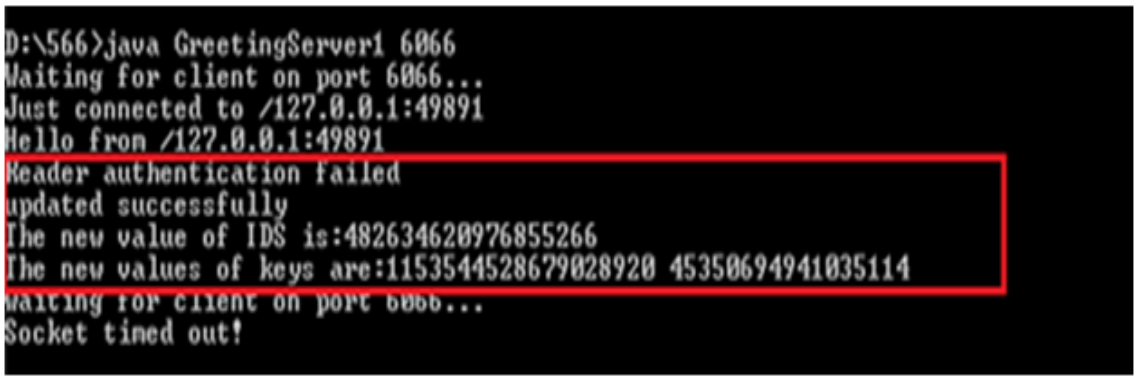


Figure 4.2: Modified RAPP Tag side

present in the database of the reader, the values of secrets fetched by the tag and the reader mismatch and the authentication between them permanently fails. From the simulation, different values of keys at the tag and the reader side can be seen.

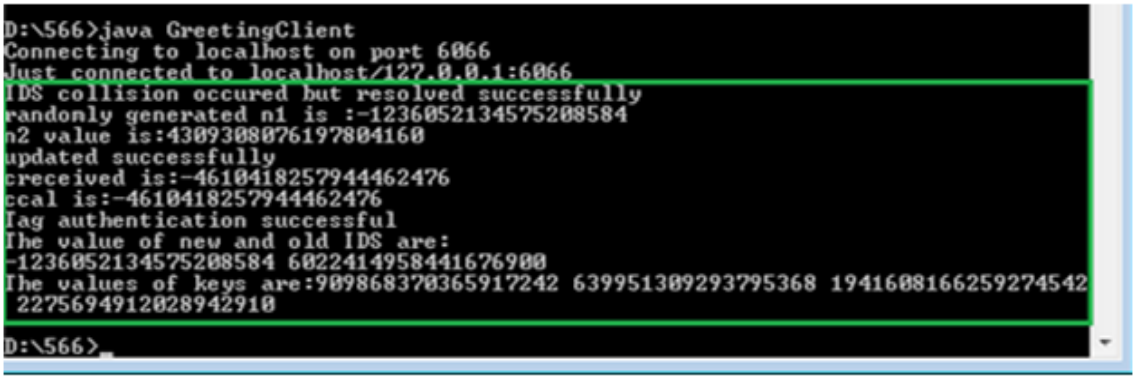


Figure 4.3: Reader side execution of RAPP when prone to IDS collision attack.

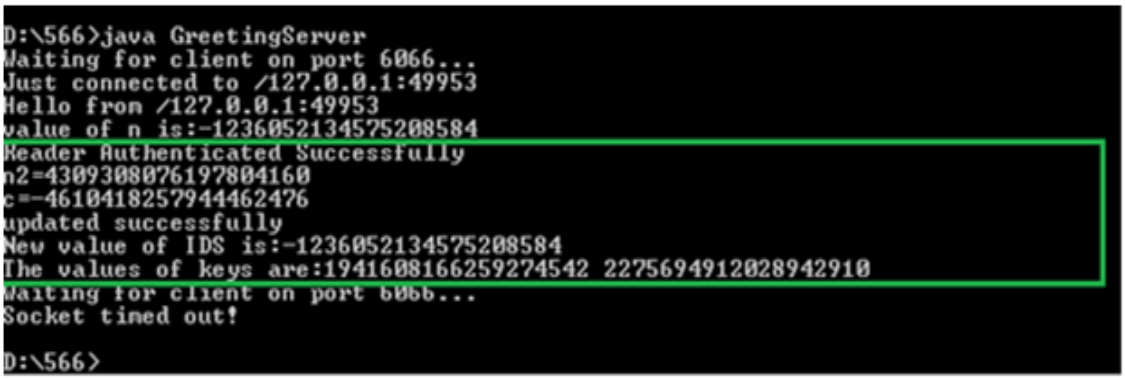


Figure 4.4: Tag side execution of RAPP when prone to IDS collision attack.

In the new RAPP authentication algorithm after proposing the required modifications, when IDS for the next session is generated, it is checked against the reader's database to find out if it is already present or not. If it is already present, a new value of IDS will be generated and used.The simulation result, shows how the IDS collision attack occurred and is resolved in the new protocol.

4.2 Simulation of RFID authentication protocol using shufflebits

Simulation result of one round of authentication of RFID authentication protocol using Shufflebits() operation is as follows:

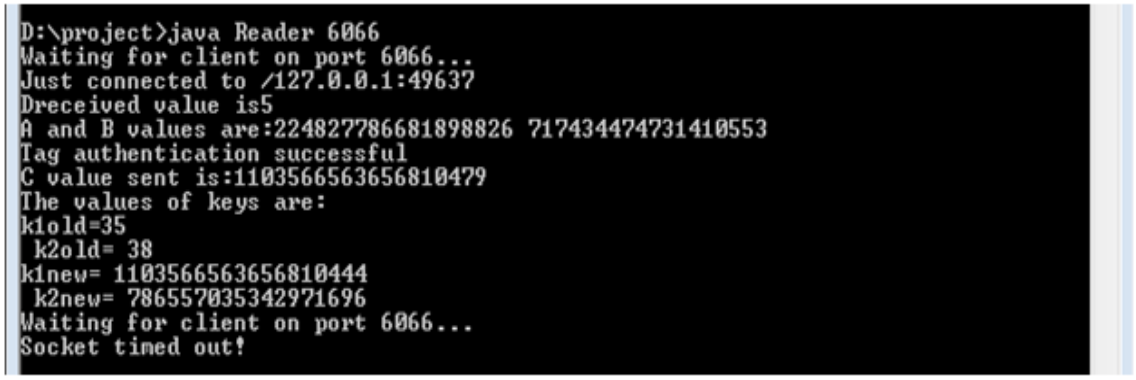


Figure 4.5: Reader side execution of RFID protocol with Shufflebits

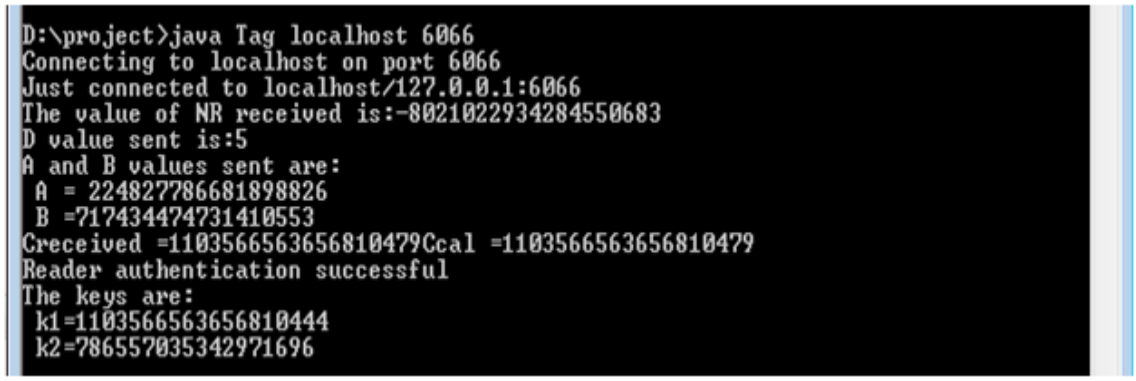


Figure 4.6: Tag side execution of RFID protocol with SHufflebits

4.3 Simulation of SIDRFID mutual authentication protocol

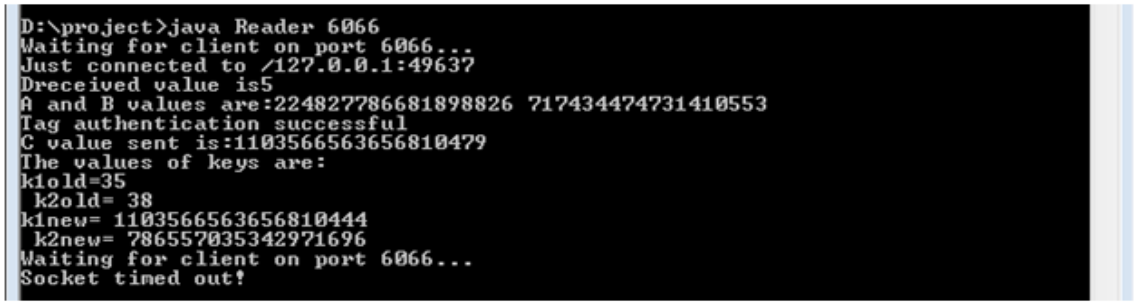


Figure 4.7: Reader side execution of SIDRFID

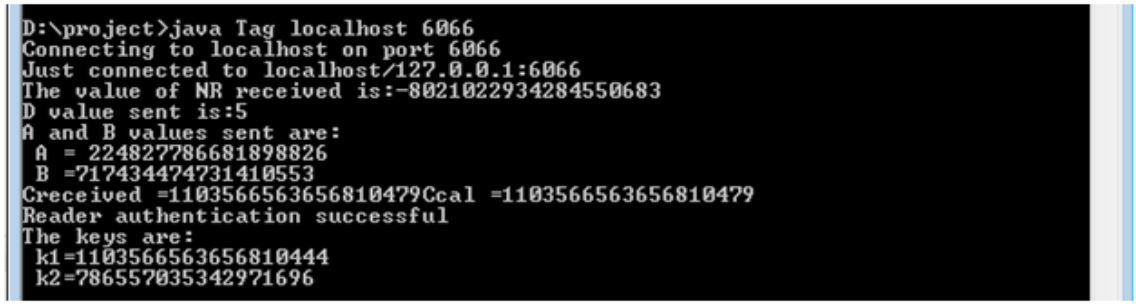


Figure 4.8: Tag side execution of SIDRFID

The comparison between the existing and the new protocol with respect to the resources required at the tag side are as follows:

Parameter	Old SIDRFID	New SIDRFID
Type of Computation operations	4 $\oplus$, 5 Rot	4 $\oplus$,5 Halfrot, 2 $\vee$,2 $\wedge$
Storage requirement	2L	2L
Communication messages	4	4
Resistance to HW disclosure attack	No	Yes
Resistance to Traceability attack	No	Yes

Table 4.2: Comparison of old SIDRFID and improved SIRFID authentication protocols

4.4 Simulation of DIDRFID mutual authentication protocol

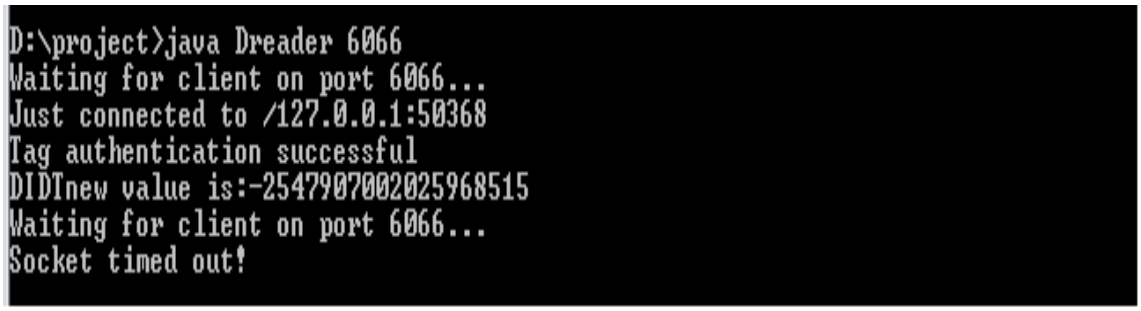


Figure 4.9: Reader side execution of DIDRFID

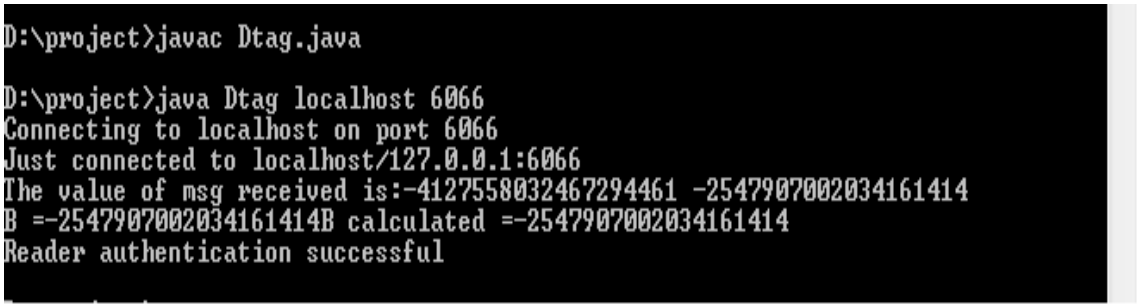


Figure 4.10: Tag side execution of DIDRFID

The comparison between the existing and the new protocol with respect to the resources required at the tag side are as follows:

Parameter	Old DIDRFID	New DIDRFID
Type of Computation operations	5⊕, 8 Halfrot,2 ∨,2 ∧	5 ⊕,8 Halfrot,4 ∨,2 ∧,2 ∼
Storage requirement	2L	2L
Communication messages	4	4
Resistance to HW disclosure attack	No	Yes
Resistance to Full disclosure attack	No	Yes

Table 4.3: Comparison of old DIDRFID and Improved SIRFID authentication protocols

4.5 Verification using SPAN animator

AVISPA(Automated Validation of Internet Security Protocol) [19] is a tool for verifying the security of large scale internet protocols. AVISPA uses a language called HLPSL(High Level Protocol Specification Language) for specifying the protocol which is more clear and more detailed compared to the traditional Alice-Bob representation of the protocol. This language is also more difficult to specify.

SPAN(Security Protocol Animator for AVISPA) [16] is a tool which uses CAS+ language for protocol specification. This language is far easy compared to the HLPSL. SPAN also has the capability of converting the CAS+ language specifications into HLPSL directly. It can also generate Message sequence charts and also can build active attacks on the specified protocol. It uses four backends for validation of the protocols namely:

1. OFMC 2.CL-ATSE 3.SATMC 4.TA4SP

The architecture of the tool is as follows:

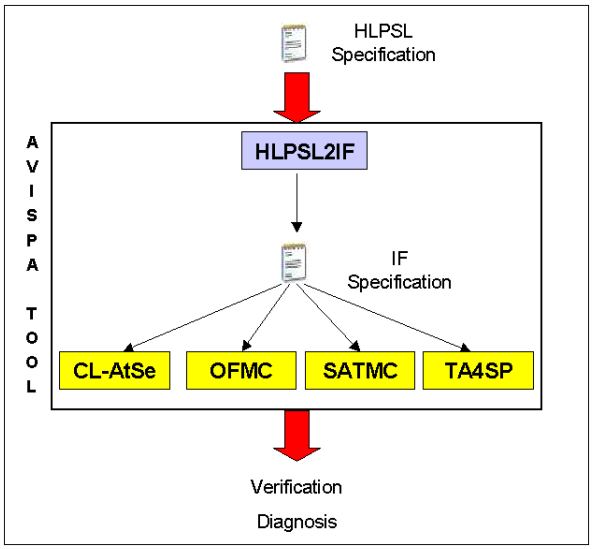
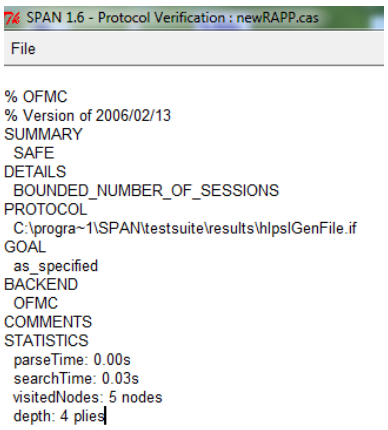
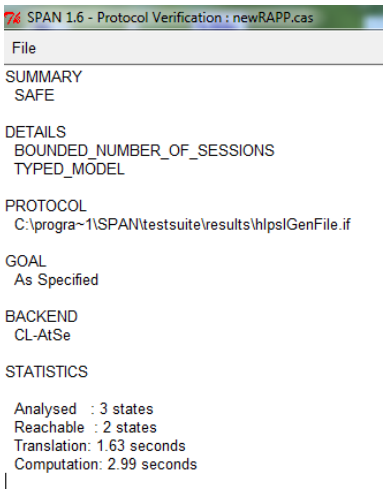


Figure 4.11: Tag side

4.5.1 Verification of Improved RAPP authentication protocol



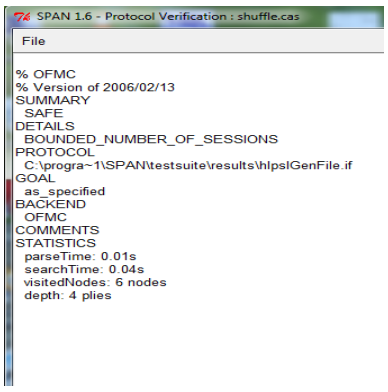
(a) Verification using OFMC



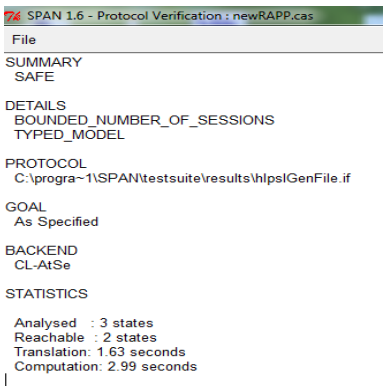
(b) verification using CL-ATSE

Figure 4.12: Verification of new improved RAPP protocol using SPAN

4.5.2 Verification of authentication protocol using shufflebits



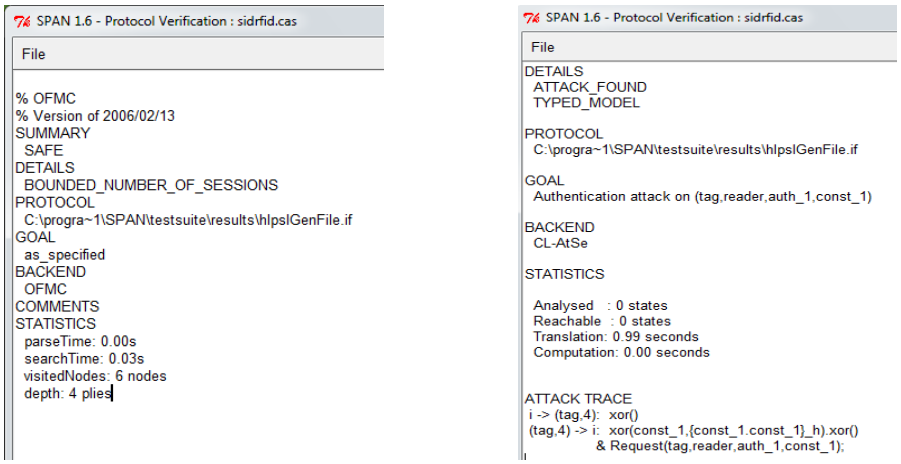
(a) Verification using OFMC



(b) verification using CL-ATSE

Figure 4.13: Verification of new RFID protocol using Shufflebits in SPAN

4.5.3 Verification of former SIDRFID authentication protocol



(a) Verification using OFMC (b) verification using CL-ATSE

Figure 4.14: Verification of original SIDRFID authentication protocol in SPAN

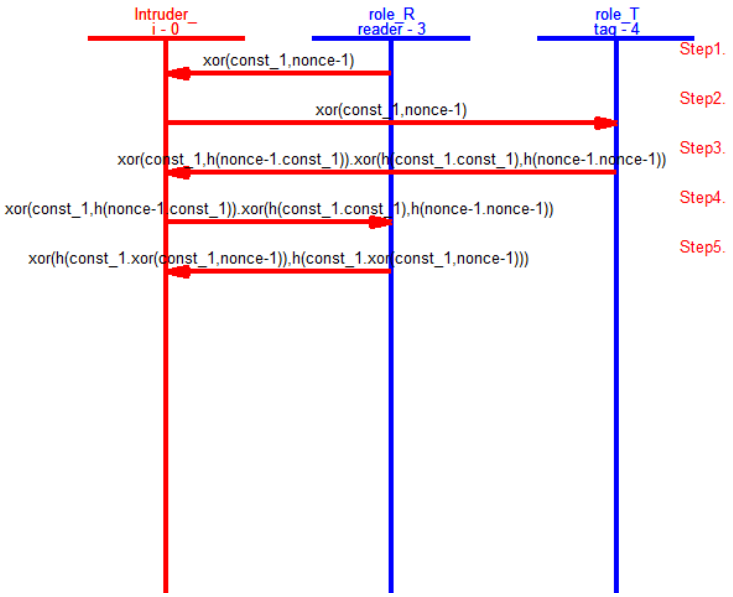
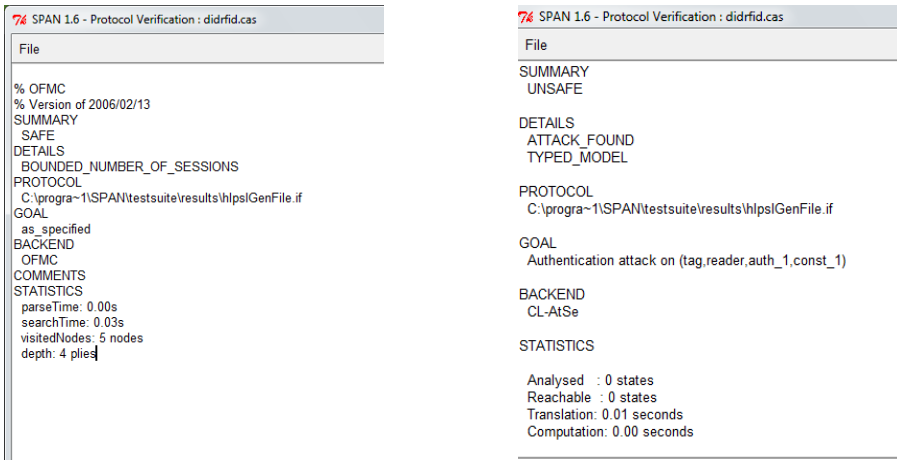


Figure 4.15: Message sequence chart for Attack trace on sidrfid protocol

4.5.4 Verification of former DIDRFID authentication protocol



(a) Verification using OFMC (b) verification using CL-ATSE

Figure 4.16: Verification of original DIDRFID authentication protocol in SPAN

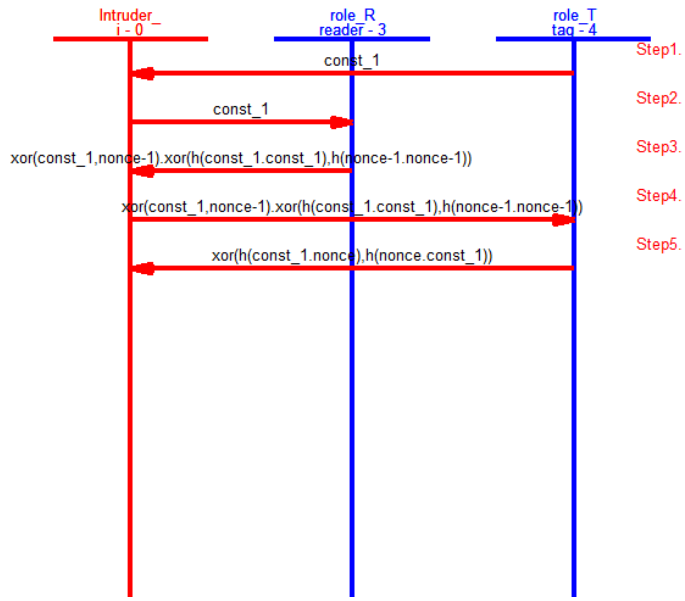
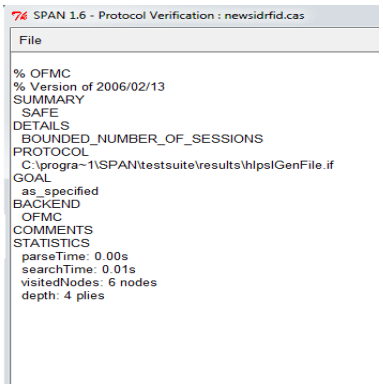
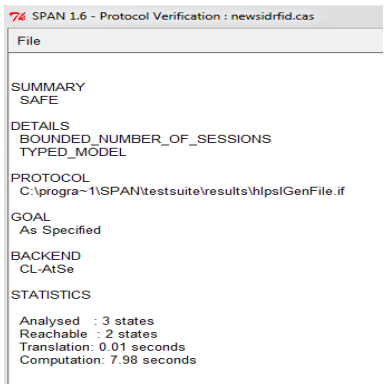


Figure 4.17: Message sequence chart for Attack trace on didrfid protocol

4.5.5 Verification of modified SIDRFID authentication protocol



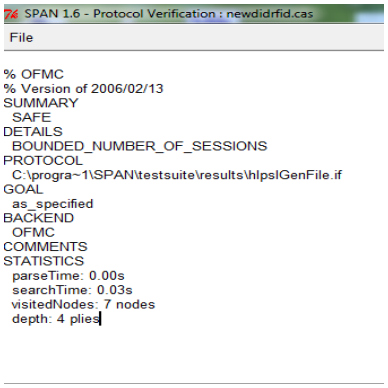
(a) Verification using OFMC



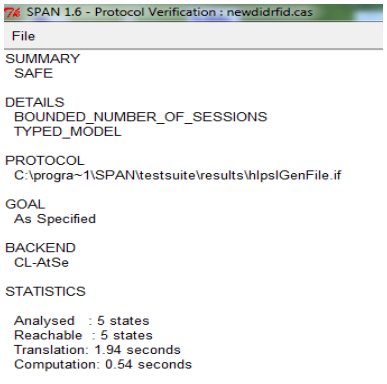
(b) verification using CL-ATSE

Figure 4.18: Verification of modified SIDRFID protocl using SPAN

4.5.6 Verification of modified DIDRFID authentication protocol



(a) Verification using OFMC



(b) verification using CL-ATSE

Figure 4.19: Verification of modified DIDRFID protocol using SPAN

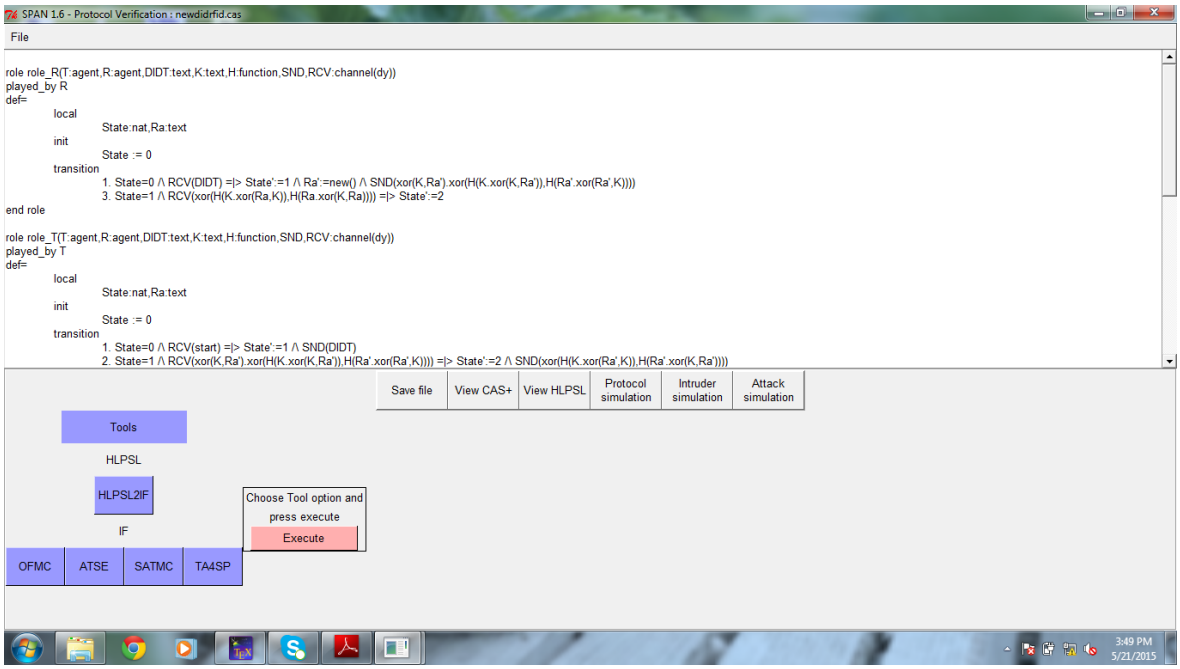


Figure 4.20: SPAN screen

Protocol	OFMC	CL-ATSE
Improved RAPP	SAFE	SAFE
RFID protocol using Shufflebits	SAFE	SAFE
Old SIDRFID	SAFE	UNSAFE
New SIDRFID	SAFE	SAFE
Old DIDRFID	SAFE	UNSAFE
New DIDRFID	SAFE	SAFE

Table 4.4: Comaparison of security of various protocols as determined by SPAN

Chapter5

Conclusion

IoT is gaining importance tremendously with its wide range of applications. The use of RFID technology which is very useful in establishment of IoT , is also increasing parallelly. So, the the problems with security and privacy associated with this technology should be carefully addressed. RFID tags come with different specifications and design.Low cost and passive RFID tags donot have enough resources associated with them to perform standard cryptographic functions like complex hash functions, pseudo random generator functions etc. So, to use RFID technology for IoT, we need to design minimal cost authentication protocols while ensuring that the required security goals are achieved. We also need to consider the limitations of this technology.

In this thesis, we have considered few authentication protocols suitable for low cost passive RFID tags and analysed their security properties and proposed modifications to them.We have also designed a new authentication protocol that makes use of Shufflebits operation.From the simulation results and the verification using the SPAN animator, it can be concluded that the proposed new protocols are resistant to the attacks which could not be handled by the former protocols. The proposed protocols compared to their original ones provide improved security features. The new protocols use better techniques for providing the security. So, this infers that the objective of our project to design robust authentication protocols using the minimal resources on RFID tags is achieved.

Scope for Further Research

In future new authentication protocols can be proposed that are more robust and secure, consumes minimum resources on tags and requires minimum data storage.

Bibliography

[1] Y. Tian, G. Chen, and J. Li. "A new ultralightweight RFID authentication protocol with permutation". IEEE Communications Letters,vol 16(5) pp 702-705, 2012.

[2] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref. "Desynchronization attack on RAPP ultralightweight authentication protocol".Cryptology ePrint Archive, Report 2012/490, 2012.

[3] I. S. Jeon and E. J. Yoon, "Cryptanalysis and Improvement of a New Ultra-lightweight RFID Authentication Protocol with Permutation", Applied Mathematical Sciences, Vol. 7, No. 69, pp. 3433-3444, 2013.

[4] S.H. Wang, Z. Han, S. Liu, and D.-W. Chen." Security analysis of RAPP an rfid authentication protocol based on permutation".Cryptology ePrint Archive, Report 2012 vol.327, 2012.

[5] Zeeshan Bilal, Keith Martin and Qasim Saeed,"Multiple attacks on Authentication protocols for low cost RFID tags".An international journal on Applied Mathematics and sciences,vol.9,no.2,pp.561-569,2015.

[6] G. Avoine and X. Carpent, Yet Another Ultralightweight Authentication Protocol that is Broken, in Radio Frequency Identification. Security and Privacy Issues. Nijmegen,Netherlands: Springer, pp. 20-30,2013.

[7] Lee Y.C., Two Ultra lightweight Authentication Protocols for Low-Cost RFID Tags, Applied Mathematics and Information Sciences, vol. 6, no. 2, pp. 425-431, 2012.

[8] Bilal.Z, Masood. A, Kausar, Firdous,"Security Analysis of Ultra-lightweight Cryptographic Protocol for Low-cost RFID Tags: Gossamer Protocol",International conference on Network based information systems(NBIS'09), Indianapolis, vol 768,pp. 260-267,2009.

[9] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador, and A. Ribagorda,M^2AP: A minimalist mutual-authentication protocol for lowcost RFID tags, in Proc.International Conference on Ubiquitous Intelligence and Computing, pp. 912-923,2006.

[10] H.Y. Chien, SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity, IEEE Trans.Dependable and Secure Computing, vol. 4, no. 4, pp. 337-340, Oct.-Dec.2007.

[11] R. C. W. Phan, Cryptanalysis of a new ultralightweight RFID authentication protocolSASI, IEEE Trans. Dependable and Secure Computing, vol. 6, no. 4, pp. 316-320, Oct.-Dec. 2009.

[12] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador, and A. Ribagorda, Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol, in Proc.of International Workshop on Information Security Applications, pp. 56-68,2008.

[13] Rolf H. Weber,"Internet of Things New security and privacy challenges", computer law and security review,elsevier journal,Volume 26, Issue 1,pp 23-30,january 2010.

[14]]. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda."LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags". Workshop on RFID Security (RFIDSEC'06),pages 6, 2006.

[15] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda." EMAP: An efficient mutual authentication protocol for low-cost RFID tags". in Proc. of Internet Systems06, volume 4277 of Lecture notes in computer sciecne, pages 352-361. Springer-Verlag, 2006.

[16] http://www.irisa.fr/celtique/genet/span/manual.pdf

[17] Rima Hussin Embrak Alakrut, Azman Samsudin and Alfin Syafalni,"Provably Lightweight RFID Mutual Authentication Protocol ",International Journal of Security and Its Applications ,Vol. 7, No. 4, July, 2013.

[18] Salekul Islam, "Security Analysis of LMAP using AVISPA",International journal of security and networks,vol.9,No. 1 ,pp 30-39 ,2014.

[19] The AVISPA Team (2006) AVISPA v1.1 User Manual, Document Version: 1.1.

[20] A. Juels, RFID Security and Privacy: A Research Survey, The IEEE Journal on the Selected Areas in Communications, Vol. 24, No. 2, FEBRUARY 2006

[21] Xinying Zheng,Chien-Ming Chen,Tsu-Yang Wu,"Another Improvement of RAPP: An Ultra-lightweight Authentication Protocol for RFID",Advances in Intelligent Systems and Computing Volume 297,pp 145-153.Springer-Verlag,2014.

Bibliography

[1] T. Leinmuller, E. Schoch, and F. Kargl. Position verification approaches for vehicular ad hoc networks. *Wireless Communications, IEEE*, 13(5):16–21, 2006.